



$H \subset G$ ss-gpe si $H \neq \emptyset$ et $\forall x, y \in H \quad xy^{-1} \in H$

Thm: Les sous-groupes de $(\mathbb{Z}, +)$ sont $n\mathbb{Z}$ avec n fixe.

pr: Obs $n\mathbb{Z} := \{nk : k \in \mathbb{Z} \text{ qlcq}\}$ c'est un ss-gpe $\neq \emptyset$ $0 \in n\mathbb{Z}$

$$\begin{aligned} y &= nk & y^{-1} &= ? -nk & xy^{-1} &= x-y = nk-nl = n(k-l) \in n\mathbb{Z} \\ y &= nk \end{aligned}$$

Soit $H \subset \mathbb{Z}$ un ss-gpe qlcq $H \neq \emptyset$ $1 \in H$, càd $0 \in H$

$$\text{Si } H = \{0\}, \quad H = 0\mathbb{Z}$$

Si non $\exists h \in \mathbb{Z} \cap H, \quad h \neq 0$ $\text{ " } h^{-1}$

Quitte à repl $h \mapsto -h \in H$

$\forall h \in H \quad h^{-1} \in H \quad \text{c}=\text{x} \quad y = h \text{ dif}$

Donc OPS $h \geq 1$

$n := \min \{h \in H : h \geq 1\} \neq \emptyset \quad E \subset \mathbb{N} \quad E \neq \emptyset$ il exist el' min

$$n \in H \leadsto n+n \in H \quad n+n+n \in H$$

$$\leadsto -n \in H, \quad -n-n \in H$$

$$\text{donc } n\mathbb{Z} \subset H$$

Aff: $H = n\mathbb{Z}$ pour ce n min

pr: Soit $a \in H$ qlcq Euclidiviser $a = qn + r$ $0 \leq r \leq n-1$

$\in H$ car $n\mathbb{Z} \subset H$

$$\Rightarrow a - qn = r \quad \text{donc } r \in H$$

Si $1 \leq r$, contradiction avec $n = \text{minimal}$

$$\text{Donc } r = 0$$

$$\text{Donc } a = qn \in n\mathbb{Z}$$

$$\text{càd } \forall a \in H \quad a \in n\mathbb{Z}$$

$$\Leftrightarrow H \subset n\mathbb{Z}$$

$$\Leftrightarrow H = n\mathbb{Z} \quad \square$$

Ex: $H = 6\mathbb{Z} \subset \mathbb{Z} = \{\dots, -18, -12, -6, 0, 6, 12, 18, 24, \dots\}$

Prop important (i) HCG ss-gre de G
(ii) $xy^{-1} \in H \quad \forall x, y \in H$

Prop: Soit $G \xrightarrow{f} G'$ morphisme de gres
HCG ss-gre de G

(1) $f(H) =: H'$ est un ss-gre de G'

(2) Si $H' \subset G'$ est un ss-gre de G' , alors

$f^{-1}(H') = \{h \in G : f(h) \in H'\}$ aussi un ss-gre de G

pr(1):

$$Im f = \{f(x) \in G' : x \in H\}$$

$$f(x)f(y)^{-1} \in Im f$$

ou i car

$$\underbrace{f(xy^{-1})}_{\in H} = f(y) \text{ pour un } y \in H$$

pr(2):

$$f(1_G) = 1_{G'}$$

$$x \in f^{-1}(H') \quad y \in f^{-1}(H') \text{ alors } f(x) \in H', f(y) \in H'$$

$$H' \text{ ss-gre} \Rightarrow f(x)f(y)^{-1} \in H'$$

$$f \text{ morph} \Rightarrow f(xy^{-1}) \in H'$$

$$\text{cà d } xy^{-1} \in f^{-1}(H') \quad \square$$

Cor *

Prop:

Le noyau $\text{Ker } f = f^{-1}(\{1_{G'}\})$

et l'image $f(G)$ sont des ss-gres G', G

car $\{1_{G'}\} \subset G'$ est un ss-gre
donc $f^{-1}(\{1_{G'}\})$ est un ss-gre
 $G \subset G$ est un ss-gre de G
 $G = G$ j'essaie.
 $f(G) =$ l'image est un ss-gre

Prop:

f inject $\Leftrightarrow \text{Ker } f = \{1_G\}$

pr:

$$f(x) = f(y) \Leftrightarrow f(x)f(y)^{-1} = 1_{G'}$$

$$\Leftrightarrow f(xy^{-1}) = 1_{G'}$$

$$\text{si } f \text{ inj: Soit } x \in \text{Ker } f \quad f(x) = 1_{G'} = f(1_G) \Rightarrow x = 1_G \quad \text{Ker } f = \{1_G\}$$

$\Rightarrow$

$$\text{si } \text{Ker } f = \{1_G\}: \text{ Soient } x, y \in G \text{ avec } f(x) = f(y) \Rightarrow f(xy^{-1}) = 1_{G'} \Rightarrow xy^{-1} = 1_G$$

$$\Leftrightarrow x = y$$

$$\text{cà d } f \text{ inj. } \quad \square$$

Def:

Soit G un gre, Soit $H \subset G$ un ss-gre.

On dit que H est distingué si

$$\forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H \quad \text{Notation}$$

cà d

$$gHg^{-1} = H \quad gH = \{gh : h \in H, g \in G\}$$

$$gHg^{-1} = \{ghg^{-1} : h \in H, g \in G\}$$

*, . REV.

On note Loi de G pas forcément

commutatif

$$H \triangleleft G$$

$\hookrightarrow H$ ss-gre de G et H distingué

$$g \in G, h \in H$$

$$H \subset G \text{ ss-gre}$$

$$j = g * h$$

$$y = j * g^{-1}$$

$$\text{si } y = h \text{ i.e. } g = g * h * g^{-1} = h$$

donc H est distingué

$$\text{Ex } \mathbb{Z} = \{\dots, -6, 0, 6, 12, \dots\}$$

$$\begin{matrix} \times 6\mathbb{Z} & \times 6\mathbb{Z} \\ 7+6+(-4) & = 6 \in 6\mathbb{Z} \end{matrix}$$

$$\in \mathbb{Z} \quad \in \mathbb{Z}$$

Anticipation

Thm: Si $H \triangleleft G \rightsquigarrow G/H$ groupe quotient

Faux si H pas distingué

Ex: $G = \mathbb{Z}, H = n\mathbb{Z} \rightsquigarrow \mathbb{Z}/n\mathbb{Z}$
distingué!

Obs: Si G est commutatif, tout ss-gpe $H \subset G$ est dist.

pv: $ghg^{-1} = gg^{-1}h = h \in H \quad \forall g \in G \quad \forall h \in H$

Obs^{exo}: $H := \{1_G\}$

e et $H := G$ sont deux ss-gpes distingués de G $\square$

Def: $\text{Ker } f \triangleleft G$ pour tout morph $G \xrightarrow{f} G'$

$\downarrow$
ss-gpe (v.u.)

pv: Soit $x \in \text{Ker } f$ Soit $g \in G$ arbitraire But: $gxg^{-1} \stackrel{!}{\in} \text{Ker } f$

$$\begin{aligned} 1_{G'} &\stackrel{!}{=} f(gxg^{-1}) \\ [x \in \text{Ker } f] &= f(g) \cdot \underbrace{f(x)}_{1_{G'}} \cdot f(g^{-1}) \\ &= f(g) \quad f(g^{-1}) \\ [f \text{ morph}] &= f(gg^{-1}) \\ &= f(1_G) = 1_{G'} \quad \text{OK } \square \end{aligned}$$

Deux ss-gpes de $\mathbb{Z} \times \mathbb{Z}$ $H_1 := \{(x, 0) : x \in \mathbb{Z}\}$
 $H_2 := \{(0, y) : y \in \mathbb{Z}\}$

$H_1 \cup H_2 \stackrel{!}{\text{ss-gpe}} \text{ NON}$

$(x, 0) + (0, y) = (x, y)$ avec $x \neq 0 \neq y$ $(x, y) \notin H_1 \cup H_2$

Pbm: Réunion de ss-gpes pas en général un ss-gpe

Partie $P \subset G$ ex $P = H_1 \cup H_2$

càd un ss-ensemble, pas forcément ss-gpe

$\langle P \rangle :=$ le ss-gpe engendré par P

$:=$ le plus petit ss-gpe de G contenant P

$\langle P \rangle$ - ss-gpe.

$\langle P \rangle$ engendré par P

$\langle P \rangle$ le plus petit ss-gpe contenant P

Obs: Si $H_i \subset G$ avec $i \in I$ famille quelq
des ss-grps, alors $\bigcap_{i \in I} H_i \subset G$ est un ss-grp de G $\square$

$\langle P \rangle := \bigcap_{P \subset H \subset G} H$ c'est un ss-grp le plus petit!

Thm: Soit $P \subset G$ une partie (ss-)ensemble

On note $P^{-1} := \{x^{-1} : x \in P\}$

Alors $\langle P \rangle := \{x_1 \dots x_n \in G : n \geq 0 \text{ entier}$
 $x_i \in P \text{ ou } x_i \in P^{-1}\}$

pv: Poser $H := \{x_1 \dots x_n : n \geq 0, x_i \in P \cup P^{-1}\}$ But $\langle P \rangle \stackrel{!}{=} H$

Aff: $H \subset \langle P \rangle$

pv: Soit $x_1 \dots x_n \in H$ avec $x_i \in P$ ou $x_i \in P^{-1}$. Comme $P \subset \langle P \rangle$, on a $x_i \in \langle P \rangle$
ou $x_i^{-1} \in \langle P \rangle$

Comme P est un ss-grp par def, il est clair

$x_1, \dots, x_n \in \langle P \rangle$

Aff: $\langle P \rangle \subset H$

pv: $\langle P \rangle =$ le plus petit ss-grp contenant P ou $\bigcap$ de tous les ss-grps
contenant P intersec.

Il suffit donc de mq H est un ss-grp contenant P
 $H \supset \{x_1 \dots x_n \in P\}$ $H \supset P$

Rappel: $H \subset G$ ss-grp si $H \neq \emptyset$ et $x, y \in H \Rightarrow xy^{-1} \in H$.

Ici $H \ni 1_G$ $n=0$ donc $H \neq \emptyset$

$x = x_1 \dots x_n \in H$ $x_i \in P$ ou $x_i \in P^{-1}$

$y = y_1 \dots y_m \in H$ $y_j \in P$ ou $y_j \in P^{-1}$

$xy^{-1} = x_1 \dots x_n y_m^{-1} \dots y_1^{-1}$ $(uv)^{-1} = v^{-1}u^{-1}$

$= z_1 \dots z_n z_{n+1} \dots z_{n+m}$ avec $z_k \in P$ ou $z_k \in P^{-1}$

$\in H$ oui

Prop: ^{Partie singleton} $\langle x \rangle$ avec $\{x\} = P$, $x \in G$
 $\langle x \rangle = \{x^m : m \in \mathbb{Z}\}$

pv: $x_1 \dots x_n$ avec $x_i \in \{x\}$ ou $x_i \in \{x^{-1}\}$ càd $x_i = x$ ou $x_i = x^{-1}$

Ex: $\underline{x x^{-1} x^{-1} x} \quad \underline{x x^{-1} x} \quad \underline{x x^{-1}} = x = x^m$ x commute avec x
 $x x^{-1} = 1_G = x^{-1} x$ $\xrightarrow{\quad \quad \quad} x^{-1}$ $\square$

$\mathbb{Z}$ ss-grps sont des $n\mathbb{Z}$
 Deux ss-grps de $\mathbb{Z}$, quelle est l'intersection?

Thm: $a\mathbb{Z} \subset \mathbb{Z}$ et $b\mathbb{Z} \subset \mathbb{Z}$ deux ss-grps de $\mathbb{Z}$
 $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a,b)\mathbb{Z}$

Aussi

$\langle a, b \rangle = \text{pgcd}(a,b)\mathbb{Z}$ Poly page 123

MIRACLE BÉZOUT

$\langle a, b \rangle = \mathbb{Z}a + \mathbb{Z}b$ $\begin{smallmatrix} aa^+bb^- \\ ++-- \end{smallmatrix}$
 $\stackrel{\text{THM}}{=} \text{pgcd}(a,b)\mathbb{Z}$
 Redonne Bézout $\text{pgcd}(a,b) = ua + vb$

$\langle \cdot \rangle \rightarrow$ engendré?

Def: Relation d'équivalence $a R b$ $a, b \in E$: ensemble, si 3 axiomes satisfaits:
 (1) Réflexivité $a R a$
 (2) Symétrie $a R b \Rightarrow b R a$ Ex: $a \equiv b \pmod n$
 (3) Transitivité ($a R b$ et $b R c$) $\Rightarrow a R c$

Def: Soit E un ensemble et R une relation d'équivalence sur cet ensemble. On note la classe d'équivalence d'un élément $a \in E$ par
 $Cl_R(a) = \{x \in E : x R a\}$ = "tous les éléments de E qui sont équivalents à a "

Ex: $Cl_{\text{mod } n}(a) = \{b \in \mathbb{Z} : b \equiv a \pmod n\}$

Prop:

(1) $a \in Cl_R(a)$ $a R a$ OK (forcément)

(2) Deux classes d'éq. qui s'intersectent sont égales:

$\emptyset \neq Cl_R(a) \cap Cl_R(b) \Rightarrow Cl_R(a) = Cl_R(b)$

Eno

(3) Ou bien $Cl_R(a) = Cl_R(b)$ ou bien $Cl_R(a) \cap Cl_R(b) = \emptyset$

(4) Pour a, b

$Cl_R(a) = Cl_R(b) \Leftrightarrow a \in Cl_R(b) \Leftrightarrow b \in Cl_R(a)$

$Cl_R(a) = Cl_R(b)$ ou $Cl_R(a) \cap Cl_R(b) = \emptyset$

rv (2): Si $\exists x \in \mathcal{C}_R(a) \cap \mathcal{C}_R(b)$
 càd aRx et xRb
 Alors, pour $y \in \mathcal{C}_R(a)$ arbitraire
 $(yRa \text{ et } aRx) \Rightarrow (yRx \text{ et } xRb)$
 $\Rightarrow yRb$ càd $y \in \mathcal{C}_R(b)$
 donc $\mathcal{C}_R(a) \subset \mathcal{C}_R(b)$
 Inclusion inverse: preuve similaire
 CCL: $\mathcal{C}_R(a) = \mathcal{C}_R(b)$

Def: Une partition de E , c'est $E = \bigcup_{i \in I} A_i$ $A_i \subset E$ ss-ensemble avec
 $A_i \cap A_j = \emptyset \quad \forall i \neq j$
 $A_i \neq \emptyset \quad \forall i$

Thm: Pour une rel^o d'eq. R sur un ens. E , on a la partition:

$$E = \bigcup_{i \in I} \mathcal{C}_R(a_i) \quad \text{certains } a_i \in E$$

Ex: $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

Notation: G gr^e $H \subset G$ ss-gr^e $(G, *)$ pas forc^é commutatif
 pour $a \in G$ noter $aH := \{ah : h \in H\}$
 $H_a := \{ha : h \in H\}$

$$(x^{-1}y)^{-1} \in H^{-1} = H \\ = y^{-1}x \text{ pareil}$$

Def: La relation $x \sim_g y$ déf par $x^{-1}y \in H$ } sont d'équivalence
 gauche } irréductible
 La relation $x \sim_d y$ déf par $yx^{-1} \in H$ } l'une à l'autre
 droite

rv $\sim$: (1) $x \sim_g x$ si $x^{-1}x = 1_G \in H$ OK
 (2) $x \sim_g y$ càd $x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} \in H^{-1} = H$ ss-gr^e
 càd $y^{-1}x \in H$ càd $y \sim_g x$
 (3) $(x \sim_g y \text{ et } y \sim_g z) \Rightarrow (x^{-1}y \in H \text{ et } y^{-1}z \in H)$
 $\Rightarrow \underline{x^{-1}y} \underline{y^{-1}z} \in H$ u, v $\in H \Rightarrow uv \in H$ ss-gr^e
 càd $x^{-1}z \in H$ càd $x \sim_g z$!

Classes d'équivalences sur E
 distinctes forment une
 partition de E

pas de symbole $\cdot$ pour $u \cdot v$

Obs: Si $(G, *)$ commutatif $u \cdot v = v \cdot u \quad \forall u, v \in G$, alors $x \sim y \Leftrightarrow x \sim_d y$

Notation: $G/H := \{\bar{x} : x \in G\}$ classes d'éq à gauche mod H
 $H \backslash G := \{\bar{y}^d : y \in G\}$ droite il est égal
Il commutatif

Ex: $\mathbb{Z}/n\mathbb{Z}$ m classes à gauche et à droite

Prop: Pour tous $x, y \in G$

$$x \sim y \Leftrightarrow x^{-1} \sim_d y^{-1}$$

$$u \sim v \stackrel{\text{def}}{=} uv^{-1} \in H$$

nv:

$$\begin{aligned} x^{-1}y \in H &\Leftrightarrow (x^{-1}y)^{-1} \in H^{-1} = H \\ &\Leftrightarrow y^{-1}(x^{-1})^{-1} \in H \\ &\Leftrightarrow y^{-1} \sim_d x^{-1} \\ &\Leftrightarrow x^{-1} \sim y^{-1} \quad \square \end{aligned}$$

CCL: L'application d'inversion:

$$\begin{aligned} (\cdot)^{-1} : G/H &\longrightarrow H \backslash G \\ \bar{x} &\longmapsto \bar{x}^{-1} \end{aligned}$$

est bijective

Cor: # classes d'éq gauche = # classes d'éq droite

Notation: $\{y \in G : x \sim y\} = \bar{x}$

$$\begin{aligned} &= \{y \in G : x^{-1}y \in H\} \\ &= \{y \in G : \exists h \in H \quad x^{-1}y = h\} \\ &= \{y : y = xh\} \\ &= xH \end{aligned}$$

CCL: $\bar{x}^* = x^*H$
 $\bar{x}^d = Hx^*$

Ex: $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$
 $\bar{k} = k + n\mathbb{Z} = k^* + n\mathbb{Z}$

$[G:H]$ le nombre
de classes d'équivalence

Déf: L'indice d'un ss-grp $H \subset G$ c'est:

$$[G:H] := \text{Card classes (à gauche ou à droite) modulo } H \\ = \text{"auto-iso"}$$

Ex:

$$[\mathbb{Z}:n\mathbb{Z}] = |\mathbb{Z}/n\mathbb{Z}| = n$$

Prp: Pour $H \subset G$ ss-grp les ptes sont équivalents

(i) $H \triangleleft G$ est distingué

$$(i:) xH = Hx \quad \forall x \in G$$

$$(ii:) xHx^{-1} = H \quad \forall x \in G$$

Alors classes à gche et classes à dtes coïncident.

Thm: Si $K \subset H \subset G$ ss-grps, alors $[G:K] = [G:H] \cdot [H:K]$

Thm de Lagrange: Soit G un grp avec $|G| = \text{Card } G < \infty$ fini:

Alors pour tout ss-grp $H \subset G$ on a $|G| = [G:H] \cdot |H|$

d'où $|H| \mid |G|$
divise

pv: Poser $z := [G:H] = \# \text{ classes mod } H$
Représentants $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_z$ de ces z classes
càd $x_1H, x_2H, \dots, x_zH$

Disjointes donc

$$G = x_1H \cup x_2H \cup \dots \cup x_zH$$

$$|G| = |H| + |H| + \dots + |H| = z|H| = [G:H] \cdot |H|$$

□

Lm: $|xH| = |H| \quad \forall x \in G$ fixé

pv: $H \rightarrow xH$ Bijection d'inverse
 $h \mapsto xh$

$$\begin{array}{ccc} H & \xleftarrow{\quad} & xH \\ x^{-1}h & \xleftarrow{\quad} & h \end{array}$$

□

